BARBOSA
SOCIEDADE DE ADVOGADOS

POLÍTICA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Março de 2024

Praça Santos Dumont 70/ 2º andar - Gávea
Rio de Janeiro/RJ - CEP 22470-060

Rua Pedroso Alvarenga, 990 / 5º andar - Itaim Bibi
São Paulo/SP - CEP 04531-004

Sumário

1. Objetivo

Esta Política de Privacidade e Segurança da Informação ("Política") disciplina as normas referentes à segurança da informação no contexto das atividades desempenhadas por Barbosa Sociedade de Advogados ("Escritório").

2. Abrangência

As normas previstas nesta Política são aplicáveis a todos os colaboradores do Escritório, incluindo sócios, advogados, estagiários, funcionários, fornecedores e prestadores de serviços que tenham acesso a quaisquer Informações (conforme abaixo definido) ou Recursos Computacionais (conforme abaixo definido).

3. Preceitos

Conforme a definição da norma NBR ISO/IEC 17799:2005, a informação é um ativo que tem valor para a organização e deve ser adequadamente protegida. A segurança da informação é caracterizada pela preservação dos seguintes preceitos:

- *Confidencialidade*: garante que a informação seja acessível somente por pessoas autorizadas, pelo período necessário.
- *Disponibilidade*: garante que a informação esteja disponível para as pessoas autorizadas sempre que necessário.
- *Integridade*: garante que a informação esteja completa, íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de uso.

Para assegurar a observância desses preceitos, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

4. Definições

Para fins desta Política, as definições abaixo têm o seguinte significado:

- *Administração*: qualquer dos sócios administradores do Escritório.
- *Informação*: quaisquer Informações ou documentos a que os Usuários tenham acesso em razão do exercício de suas atividades no Escritório.
- *Recursos Computacionais*: conjunto de equipamentos, sistemas e serviços de tecnologia da informação (TI) do Escritório, incluindo aplicativos e periféricos do Escritório.
- *Usuários*: todos os colaboradores do Escritório, incluindo sócios, advogados, estagiários, funcionários, fornecedores e prestadores de serviços que utilizam os Recursos Computacionais.
- *Senha Forte*: senhas com mais de 7 caracteres formadas pela combinação de letras maiúsculas, minúsculas, números e caracteres especiais.

5. Diretrizes

5.1. As Informações (independente do formato que estejam) e os Recursos Computacionais utilizados pelos Usuários são de exclusiva propriedade do Escritório.

5.2. As Informações do Escritório, de seus clientes e do público em geral devem ser tratadas de forma ética e sigilosa, evitando-se mau uso, exposição indevida ou riscos desnecessários de exposição. Todas as Informações obtidas pelos Usuários no desempenho de suas funções no Escritório são confidenciais. Os Usuários deverão proteger essas Informações e não irão divulgá-las a outras pessoas além dos próprios Usuários envolvidos na execução dos trabalhos para os quais as Informações são utilizadas, salvo se suas funções, a lei ou a regulamentação exigirem essa divulgação e, no primeiro caso, desde que a divulgação seja autorizada pela lei ou pela regulamentação.

5.3. A informação deve ser utilizada de forma transparente e exclusivamente para a finalidade para a qual foi coletada.

5.4. Todo processo, sempre que possível, deve garantir a segregação de funções, por meio da participação de mais de uma pessoa ou equipe.

5.5. Todos os Usuários devem ter ciência de que o uso das Informações e dos Recursos Computacionais pode ser monitorado e auditado, e que os registros obtidos em razão desse monitoramento (incluindo mensagens e gravações telefônicas) poderão ser utilizados para a detecção de violações da Política de Segurança da Informação, podendo servir de evidência para a aplicação de medidas disciplinares, processos administrativos ou legais.

5.6. O acesso às Informações e aos Recursos Computacionais somente deve ser feito se devidamente autorizado. A autorização de acesso compete à Administração, observado o critério de "menor privilégio", no qual os usuários têm acesso somente às Informações e aos Recursos Computacionais imprescindíveis para o pleno desempenho de suas atividades.

5.7. A identificação de qualquer Usuário deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas a partir dos acessos utilizando a correspondente identificação.

5.8. A senha de acesso às Informações e aos Recursos Computacionais é pessoal e intransferível, devendo ser mantida secreta e sendo proibido seu compartilhamento. As senhas de todos os Usuários devem seguir as orientações fornecidas quando do acesso inicial e observar o recadastramento regular e o uso de recursos avançados de proteção como, por exemplo, autenticação de múltiplo fator. Os Usuários que não se sentirem suficientemente informados sobre como criar e seguramente utilizar suas senhas devem solicitar orientação à Administração do Escritório.

5.9. Os riscos de exposição ou destruição de Informações devem ser imediatamente reportados à Administração.

5.10. O Escritório deve prover orientação e treinamento a todos os Usuários. Devem ser realizadas orientações técnicas iniciais para novos Usuários contratados, assim como orientações

regulares para reciclagem e atualização de cenários de seguranças a serem feitas de forma contínua.

6. Normas e Responsabilidades

6.1. Cabe a todos os Usuários que acessam Informações e Recursos Computacionais do Escritório cumprir fielmente a Política de Segurança da Informação, buscar orientação dos sócios em caso de dúvidas relacionadas à segurança da informação, proteger as Informações contra acesso, modificação, destruição ou divulgação não-autorizados, assegurar que as Informações e os Recursos Computacionais sejam utilizados apenas para as finalidades aprovadas, cumprir as leis e os procedimentos que regulamentam os aspectos de propriedade intelectual e comunicar imediatamente ao Escritório quando do descumprimento ou violação desta política.

6.2. Cabe aos sócios cumprir e fazer cumprir esta Política, além de assegurar que os demais Usuários possuam acesso a essa documentação e conheçam integralmente seus termos, e comunicar imediatamente eventuais casos de violação de segurança da informação.

6.3. Cabe aos prestadores de serviços de TI gerenciar a operação de TI visando primeiramente a segurança das Informações e dos Recursos Computacionais, além de buscar as melhores condições para o correto funcionamento dos recursos de contingência como *backups*, sites alternativos e serviços secundários.

6.4. Cabe à Administração definir os níveis de acesso necessários para as atividades de cada Usuário envolvido na operação, assim como assegurar que as necessidades de alteração nos permissionamentos identificadas sejam prontamente executadas, principalmente nos casos de remoção de acessos. Os casos de cancelamento de acesso devem ser priorizados e, se possível, agendados com antecedência.

6.5. Cabe à Administração propor ajustes, melhorias e modificações desta Política e de suas normas e procedimentos.

6.6. O Escritório atua em consonância com seu Código de Ética e Conduta, com as leis federais, estaduais, municipais, normas aplicáveis da Ordem dos Advogados do Brasil, normas de segurança da informação previstas pelo Comitê de Gestão da Internet Brasil, assim como com as normas de proteção de dados previstas na Lei Geral de Proteção de Dados - LGPD.

6.7. O Escritório deverá prover Recursos Computacionais adequados para o pleno desempenho das atividades dos profissionais responsáveis por sua operação.

6.8. Ao iniciar a utilização dos equipamentos e o acesso às Informações, os Usuários atestam conhecer a Política de Segurança da Informação e declaram estar cientes de suas responsabilidades.

6.9. É responsabilidade dos Usuários manter seus equipamentos em condições normais de uso, respeitando as configurações entregues pelo Escritório e em bom estado de conservação. Os equipamentos deverão ser desligados sempre que não estiverem sendo utilizados.

6.10. É responsabilidade dos Usuários manter seus equipamentos e softwares atualizados conforme as orientações recebidas do Escritório.

6.11. Todos os acessos deverão respeitar os limites de utilização e a integridade de suas credenciais e senhas.

6.12. É responsabilidade dos Usuários manter suas senhas adequadas aos padrões estabelecidos pelo Escritório com o uso de Senha Forte. Os Usuários serão responsáveis por manter suas senhas em sigilo e não poderão compartilhá-las sob nenhuma hipótese.

6.13. O conceito do “menor acesso possível” deverá ser sempre observado. Caso o Usuário perceba que possui acessos não necessários ao desenvolvimento de seus trabalhos deverá notificar imediatamente a Administração, a qual, por sua vez, deverá providenciar o ajuste de permissionamento.

6.14. O acesso à rede de arquivos requer a habilitação de recursos avançados de autenticação, a saber, a autenticação de múltiplo fator - MFA.

6.15. Todos os arquivos contendo Informações operacionais deverão ser armazenados na rede local disponibilizada pelos servidores de arquivos do Escritório. Nenhum outro local deverá ser utilizado para armazenamento sem que haja a prévia autorização da Administração.

6.16. O armazenamento em nuvem poderá ser realizado através do uso do aplicativo OneDrive disponibilizado a todos os Usuários. O Usuário não deverá utilizar serviços pessoais ou serviços que não tenham sido contratados pelo Escritório sem prévia autorização.

6.17. O acesso a serviços de e-mail através dos Recursos Computacionais é exclusivo para contas corporativas. Toda comunicação profissional deverá ser realizada exclusivamente através de endereços de e-mail do Escritório. É vedado o envio de quaisquer Informações ou documentos por meio de e-mails pessoais. Para casos especiais de acesso, uma solicitação deverá ser enviada para a análise da Administração.

6.18. O serviço de e-mail do Escritório disponibiliza recursos de filtragem de SPAMs. É de responsabilidade dos Usuários verificar os e-mails marcados como SPAM validando a configuração dos filtros e fazendo os ajustes em sua conta necessários para o correto funcionamento do recurso.

6.19. A procedência de todos os arquivos recebidos deverá ser verificada pelos Usuários antes de sua abertura. Nesse processo é necessário validar o remetente do e-mail, a origem da mensagem, a coerência do recebimento da mensagem (e do anexo) pelo Usuário e de seu conteúdo a fim de assegurar que não trará nenhum risco de segurança ao equipamento em uso ou à estrutura de TI do Escritório. Caso haja qualquer dúvida em relação à legitimidade do arquivo recebido, o Usuário deverá solicitar a análise aos prestadores de serviços de TI para a verificação técnica do arquivo.

6.20. Os Usuários devem estar atentos ao recebimento de links, seja durante a navegação na internet ou por meio de e-mails. Esses links não devem ser clicados sem que se verifique que

o endereço de destino é seguro e previamente conhecido. Caso haja qualquer dúvida em relação à legitimidade do link de navegação recebido, os Usuários devem buscar suporte para a verificação técnica da URL de destino.

6.21. O Escritório somente permite a instalação de softwares e aplicativos após a prévia verificação das licenças de uso. É vedada a instalação de softwares sem o correto licenciamento e sem a prévia autorização. Cabe aos Usuários a verificação do licenciamento dos recursos que utilizam e, caso haja qualquer indício de problemas no licenciamento, a comunicação imediata à Administração. Não é permitida a instalação de softwares e aplicativos não relacionados ao desempenho das atividades profissionais necessárias à operação do Escritório.

6.22. Para prover melhor segurança à rede, os serviços de antivírus estão implantados na estrutura de TI do Escritório. Os Usuários deverão preservar a operação desse serviço e caso haja algum bloqueio originado pelo antivírus, o usuário deverá aceitá-lo e reportá-lo à Administração para a análise de segurança necessária.

6.23. É responsabilidade dos Usuários utilizar os serviços de navegação na web de forma segura. Isso significa o acesso apenas a sites conhecidos e de "boa reputação" junto aos serviços de classificação de conteúdo e junto ao mercado.

6.24. Os serviços de rede *wireless (WiFi)* internos são exclusivos para equipamentos do Escritório. Para conexão de equipamentos não pertencentes ao Escritório, ou que não tenham necessidade de acesso aos servidores, o usuário deverá sempre optar pela utilização da rede *wireless* externa (acesso de visitantes).

6.25. É altamente recomendável que os Usuários não utilizem redes wireless públicas, ou não conhecidas, para acessar Informações ou serviços corporativos.

6.26. Ao término da utilização das Informações é responsabilidades dos Usuários fazer o correto descarte dos arquivos. Assim a exclusão dos arquivos deverá ser realizada sem que haja a possibilidade de recuperação das Informações.

6.27. Cabe aos Usuários disponibilizar seus equipamentos para as atualizações dos softwares, serviços e sistemas operacionais previstos pelos fornecedores. Caso o processo de atualização requeira que os equipamentos sejam reiniciados, o Usuário deverá seguir com a reinicialização prontamente.

6.28. Os serviços de impressão são configurados conforme a definição da Administração do Escritório. Caso o Usuário tenha necessidades diferentes das previamente definidas, deverá solicitar aprovação à Administração e encaminhar a solicitação aprovada ao setor de TI para que sua configuração possa ser revista.

6.29. Cabe aos Usuários manter seus dispositivos móveis (*smartphones* ou *tablets*), corporativos ou pessoais, atualizados com as mais recentes configurações de segurança.

6.30. Os Usuários poderão utilizar serviços de mensageria instantânea ou similares desde que tenham a prévia aprovação dos sócios administradores. Conforme o tipo de informação trafegado por esse serviço pode haver a necessidade de registro das comunicações realizadas. Nesses casos os usuários deverão seguir as orientações recebidas pelos prestadores de serviços de TI para melhor garantir os registros dessas Informações.

6.31. Cabe ao Usuário utilizar os *links* de internet e os *links* de serviços de forma racional com a preocupação de limitar o tráfego à comunicação essencial para a operação do Escritório. Serviços que comumente demandam altas taxas de transferência (tais como *streaming* de vídeo ou áudio, sincronização de grandes volumes de dados, entre outros) devem ser evitados para evitar impacto na performance dos demais serviços. Caso haja a necessidade de utilização de serviços que demandem alta taxa de transferência, os mesmos deverão ser programados previamente em horários de menor impacto à operação.

6.32. Os arquivos armazenados nos servidores estão protegidos com versionamento conforme a política de *backup* estabelecida no Escritório. Caso o Usuário necessite restaurar alguma informação de um versionamento do *backup*, deverá ser enviada uma solicitação à Administração.

6.33. O Escritório deverá realizar testes periódicos de recuperação de *backups* com identificação de todas as mídias de armazenamento. Os *backups* da rede são realizados diariamente e armazenados por 30 dias.

6.34. Todos os computadores do Escritório são configurados para bloquear o acesso após um período de inatividade.

6.35. Mesmo contando com a configuração do bloqueio automático de acessos, é responsabilidade dos Usuários bloquear manualmente seus acessos quando seus equipamentos não estiverem em uso.

6.36. Caso haja a necessidade de contratação de novos Recursos Computacionais os Usuários deverão enviar a solicitação à Administração do Escritório.

6.37. É responsabilidade dos Usuários organizar seus arquivos de forma a minimizar ao máximo o risco de exposição de dados. Dessa forma os usuários deverão manter seus recursos computacionais (computadores, arquivos e dispositivos) somente com as Informações necessárias para sua operação ou com Informações que poderão ser necessárias em datas futuras.

6.38. Cabe aos Usuários comunicar aos prestadores de serviços de TI sobre problemas de funcionamento dos seus Recursos Computacionais (computador ou *software*). Contudo, é recomendável que alguns procedimentos de recuperação sejam feitos pelos Usuários antes do envio da solicitação e abertura do ticket de atendimento.

6.39. Caso o Usuário note algum evento que possa representar alguma ameaça à segurança das Informações ou dos Recursos Computacionais, deverá imediatamente comunicar à Administração. Perda de senhas, exposição de dados, acessos indevidos, recebimentos de e-mails maliciosos, avisos e alertas do antivírus são exemplos de eventos graves que devem ser imediatamente reportados pelos Usuários.

6.40. Em caso de armazenamento de dados pessoais de clientes, tais dados poderão ser excluídos ao término do contrato a pedido do contratante. Nesse caso, o arquivo de log confirmando a exclusão poderá ser solicitado e encaminhado ao cliente.

7. Disposições Finais

Esta Política foi elaborada pelos sócios do Escritório, que deverão aprovar toda e qualquer modificação ao seu conteúdo, a qual deverá ser amplamente divulgada a todas as áreas e profissionais do Escritório por e-mail com confirmação de leitura.

Esta Política deverá ser revisada anualmente ou a qualquer tempo em razão de circunstâncias que demandem tal providência.